



# SPYWOLF

## Security Audit Report



Completed on  
**May 25, 2023**

@SPYWOLFNETWORK



@SPYWOLFNETWORK



SPYWOLF.CO





# OVERVIEW

This audit has been prepared for **MIPEPE** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

*The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal*

”

- SPYWOLF Team -





# TABLE OF CONTENTS

---

Project Description	01
Contract Information	02
Current Stats	03
Vulnerability Check	04
Threat Levels	05
Found Threats	06-A/06-E
Good Practices	07
Tokenomics	08
Team Information	09
Website Analysis	10
Social Media & Online Presence	11
About SPYWOLF	12
Disclaimer	13



# MIPEPE



## PROJECT DESCRIPTION

### **According to their website:**

Mipepe represents a new paradigm where beauty and strength intertwine. Prepare to be captivated by Mipepe - The Super Girl of Magnificent Beauty and Enormous Strength.

Mipepe emerges from the realm of imagination as a captivating figure, embodying a perfect blend of extraordinary beauty and awe-inspiring power. Prepare to be enthralled as Mipepe takes center stage, captivating hearts and minds with her remarkable presence.

**Release Date:** Presale starts in May, 2023

**Category:** Meme token



# CONTRACT INFO

Token Name  
MIPEPE

Symbol  
MIPEPE

Contract Address

0xe74865Bb59C9a8802756d46329dBe27F1734E01a

Network

Binance Smart Chain

Language

Solidity

Deployment Date

May 20, 2023

Verified?

Yes

Total Supply

690,420,000,000,000

Status

Not Launched

## TAXES

Buy Tax  
**none**

Sell Tax  
**5%**

\*Taxes can be changed in future



## Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

### Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



## TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	690420000000000 MIPEPE
Median Transfer Amount	690420000000000 MIPEPE
Average Transfer Amount	690420000000000 MIPEPE
First transfer date	2023-05-20
Last transfer date	2023-05-20
Days token transferred	1

## SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2023-05-20 06:29:50 UTC
Created	2023-05-20 06:29:50 UTC
Create TX	0x3136448cb70bca6d48a842c8066926a235def5cabe2822ced0c9b9d8d9b19701
Creator	0x1f412ead1db4c192cda44e181e008a58d25f4914



# VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



# THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

## High Risk

---

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## Medium Risk

---

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

## Low Risk

---

Issues on this level are minor details and warning that can remain unfixed.

## Informational

---

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.





# FOUND THREATS

## ⚠ High Risk

Owner can blacklist address, making it impossible to sell.

```
function blacklistAddress(address account, bool value) external onlyOwner{
    require(account != uniswapV2Pair, "invalid address");
    _isBlacklisted[account] = value;
}

function _transfer(
    address from,
    address to,
    uint256 amount
) internal override {
    require(!_isBlacklisted[from] && !_isBlacklisted[to], 'Blacklisted address');
    .....
}
```

- Recommendation:
  - Considered as good practice is blacklisting addresses for bot protection purposes to be done in automatic manner.



# FOUND THREATS

## ⚠ High Risk

Owner can set max transaction limit and max wallet limit, but cannot decrease it below 5000 tokens. The value of 5000 tokens can be lower than the transaction fees associated with the transaction.

```
function setMaxTxAmount(uint256 _amount) external onlyOwner {
    require(_amount > 5000 ether, "Zero: Max transaction amount can't be 0!");
    maxTxAmount = _amount;
}

function setMaxWalletAmount(uint256 _amount) external onlyOwner() {
    require(_amount > 5000 ether, "Zero: Max wallet amount can't be 0!");
    maxWalletAmount = _amount;
}

function _transfer(address from, address to, uint256 amount) internal override {
    .....
    if (!_isExcludedFromLimits[from] && !_isExcludedFromLimits[to]) {
        require(tradingOpen, "Trading not open yet");
        require(amount < maxTxAmount, "transfer: amount exceeds the maxTxAmount");
        if (to != uniswapV2Pair) {
            require(balanceOf(to) + amount < maxWalletAmount, "TOKEN: Balance exceeds wallet size!");
        }
    }
    .....
}
```

- Recommendation:
  - Considered as good transaction limitation practice is that it is always equal or above 0.1% of total supply.



## Informational

Owner can withdraw any tokens from the contract.

When this function is present, in cases tokens sent into the contract by mistake or purposefully, contract's owner can retrieve them.

```
function retrieveStuckTokens(address tokenaddress, address recipient, uint amount) external onlyOwner {
    require(tokenaddress != address(this), "Not retrieve native tokens!");
    require(amount <= IERC20(tokenaddress).balanceOf(address(this)),
        "Insufficient balance to transfer the requested amount.");
    IERC20(tokenaddress).transfer(recipient, amount);
}

function retrieveStuckBnb(address recipient, uint amount) external onlyOwner {
    require(amount <= address(this).balance, "Insufficient balance to transfer the requested amount.");
    (bool success, ) = payable(recipient).call{ value: amount }("");
    require(success, "Address: unable to extract value");
}

function claimCharityFees() external onlyOwner {
    uint _pendingCharityFee = pendingCharityFee;
    if (_pendingCharityFee > 0)
    {
        pendingCharityFee = 0;
        super._transfer(address(this), charityAddress, _pendingCharityFee);
    }
}
```



## Informational

Owner can set buy/sell fees up to 25% combined.

When fees are above 0, there will be certain amount of tokens that will be deducted from every transaction that users make.

Deducted amount will be as much as the fees % from total amount that user had bought, sold and/or transferred.

```
function setBuyFee(uint256 _newlpfee, uint256 _newmarketingfee, uint256 _newcharityfee) public onlyOwner {
    require((_newlpfee + _newmarketingfee + _newcharityfee + sellLPFee +
    sellMarketingFee + sellCharityFee) <= maxFeePercent, "Fee exceed the maximum limit");
    buyLPFee = _newlpfee;
    buyMarketingFee = _newmarketingfee;
    buyCharityFee = _newcharityfee;
}

function setSellFee(uint256 _newlpfee, uint256 _newmarketingfee, uint256 _newcharityfee) public onlyOwner {
    require((_newlpfee + _newmarketingfee + _newcharityfee + buyLPFee +
    buyMarketingFee + buyCharityFee) <= maxFeePercent, "Fee exceed the maximum limit");
    sellLPFee = _newlpfee;
    sellMarketingFee = _newmarketingfee;
    sellCharityFee = _newcharityfee;
}

function setMaxFeePercent(uint256 _maxfee) public onlyOwner {
    require(_maxfee <= 25, "Max Fee too high");
    maxFeePercent = _maxfee;
}
```



## Informational

Owner can exclude address from fees and transaction limits.

```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(!_isExcludedFromFees[account] != excluded, "Account is already the value of 'excluded'");
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}

function excludeFromLimits(address account, bool excluded) public onlyOwner {
    require(!_isExcludedFromLimits[account] != excluded, "Account is already the value of 'excluded'");
    _isExcludedFromLimits[account] = excluded;
    emit ExcludeFromLimits(account, excluded);
}

function excludeMultipleAccountsFromFees(address[] memory accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFees[accounts[i]] = excluded;
    }
    emit ExcludeMultipleAccountsFromFees(accounts, excluded);
}

function excludeMultipleAccountsFromLimits(address[] memory accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromLimits[accounts[i]] = excluded;
    }
    emit ExcludeMultipleAccountsFromLimits(accounts, excluded);
}
```





RECOMMENDATIONS FOR

# GOOD PRACTICES

---

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

## MIPEPE

### GOOD PRACTICES FOUND

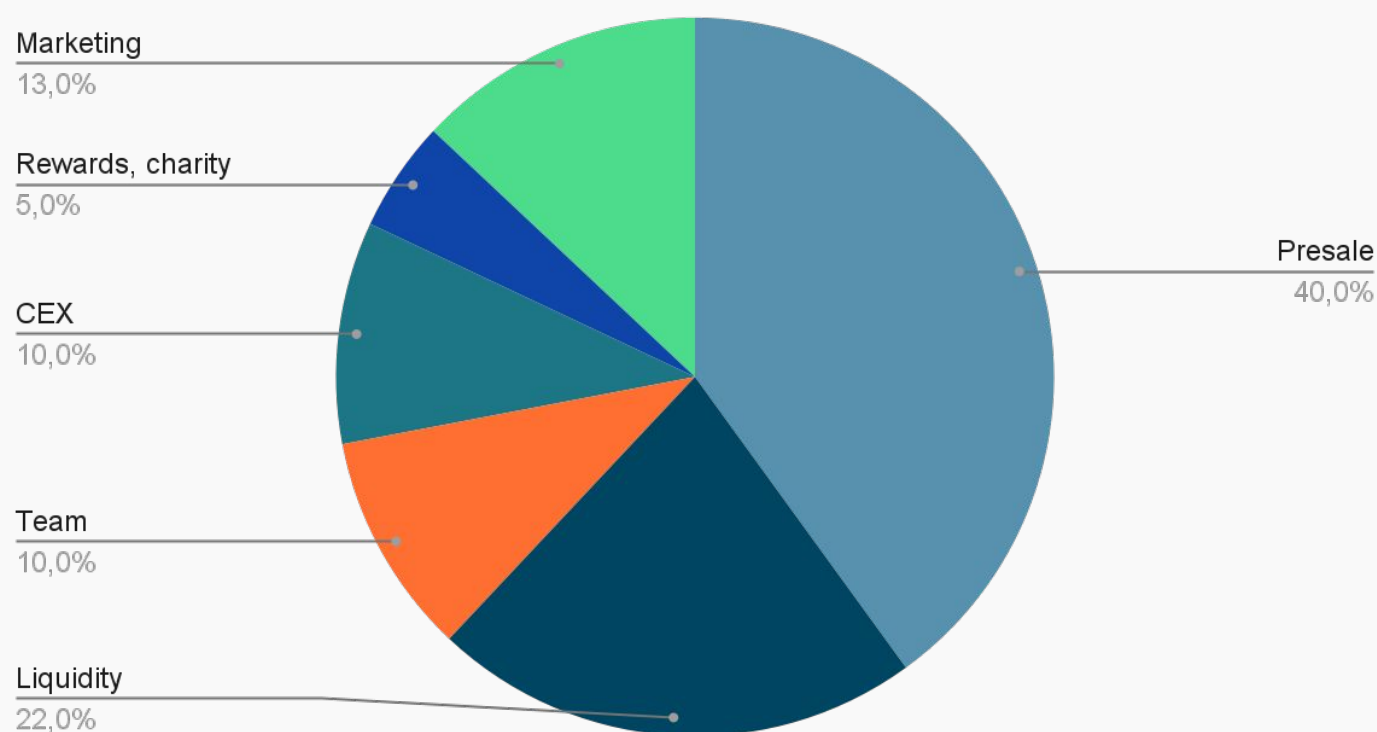
- ✓ The owner cannot mint new tokens after deployment



The following tokenomics are based on the project's whitepaper and/or website:

- 40% - Presale
- 22% - Liquidity
- 10% - CEX Listings
- 10% - Team
- 13% - Marketing
- 5% - Rewards, charity, competitions

### Tokens distribution



TOKENOMICS




# THE TEAM




## The team has privately doxxed to COINSULT

<https://coinsult.net/projects/mipepe/>


 **Coinsult**


[Projects > Project Name](#) [View chart](#) [DEXView](#)






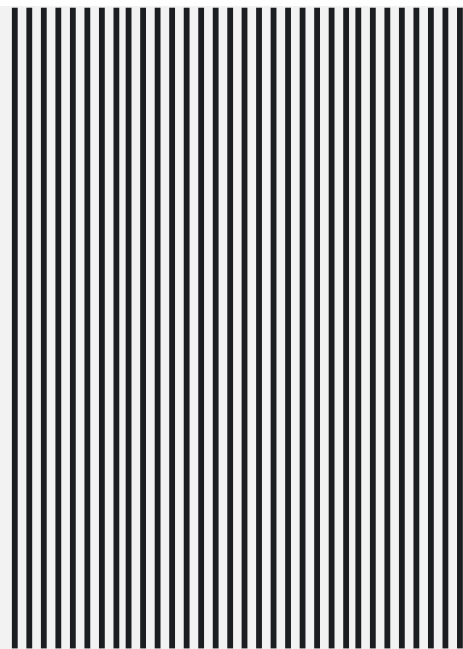
### MiPepe

Mipepe represents a new paradigm where beauty and strength intertwine. Prepare to be captivated by Mipepe - The Super Girl of Magnificent Beauty and Enormous Strength.

KYC passed 

Audit unknown 







# WEBSITE

## Website URL

<https://mipepe.vip/>

## Domain Registry

<https://www.namecheap.com>

## Domain Expiration

2024-05-18

## Technical SEO Test

Passed

## Security Test

Passed. SSL certificate present

## Design

Single page design with appropriate color scheme and graphics.

## Content

The information helps new investors understand what the product does right away. No grammar mistakes found.

## Whitepaper

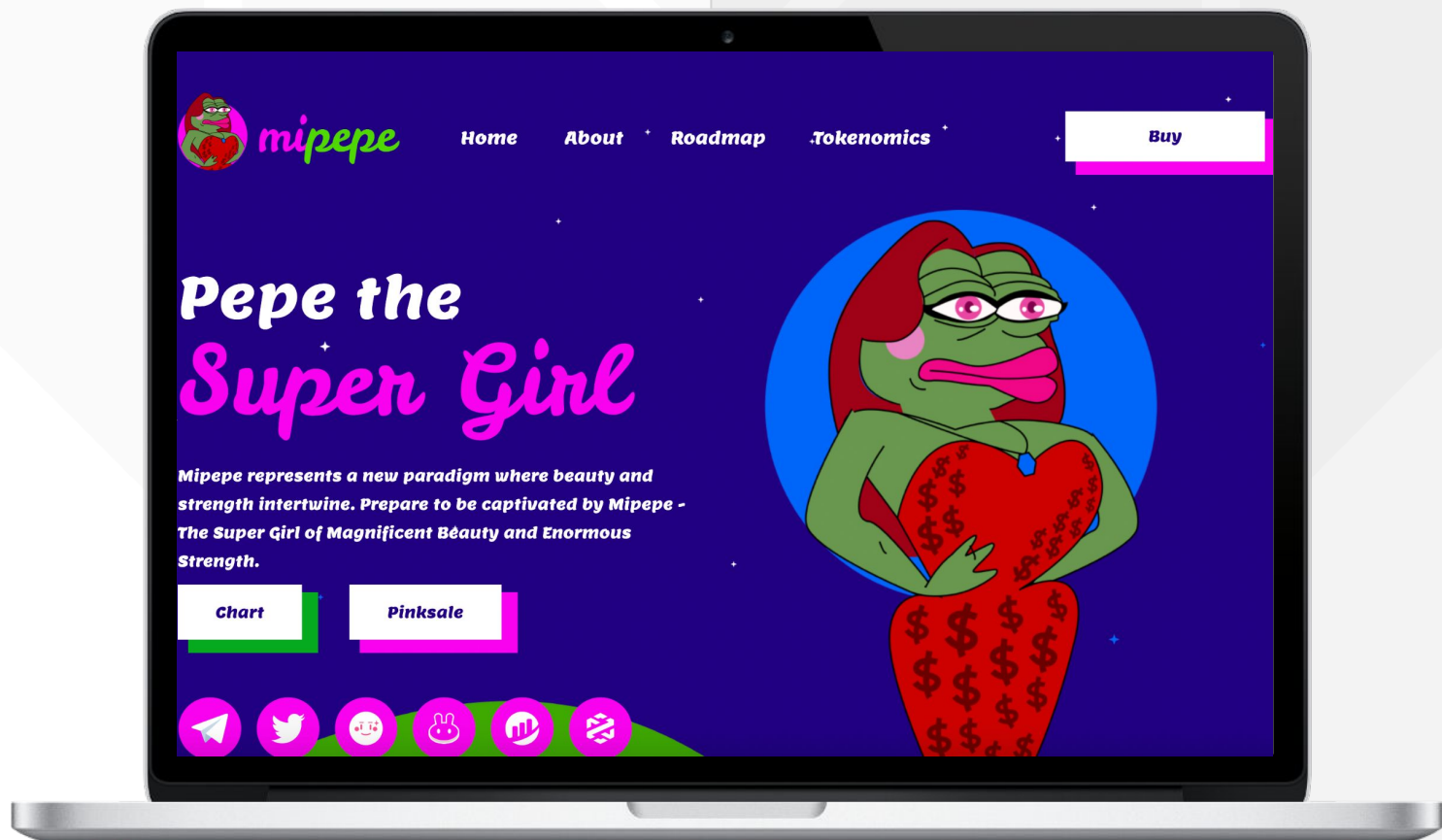
No

## Roadmap

Yes, goals set without time frames.

## Mobile-friendly?

Yes



# mipepe.vip

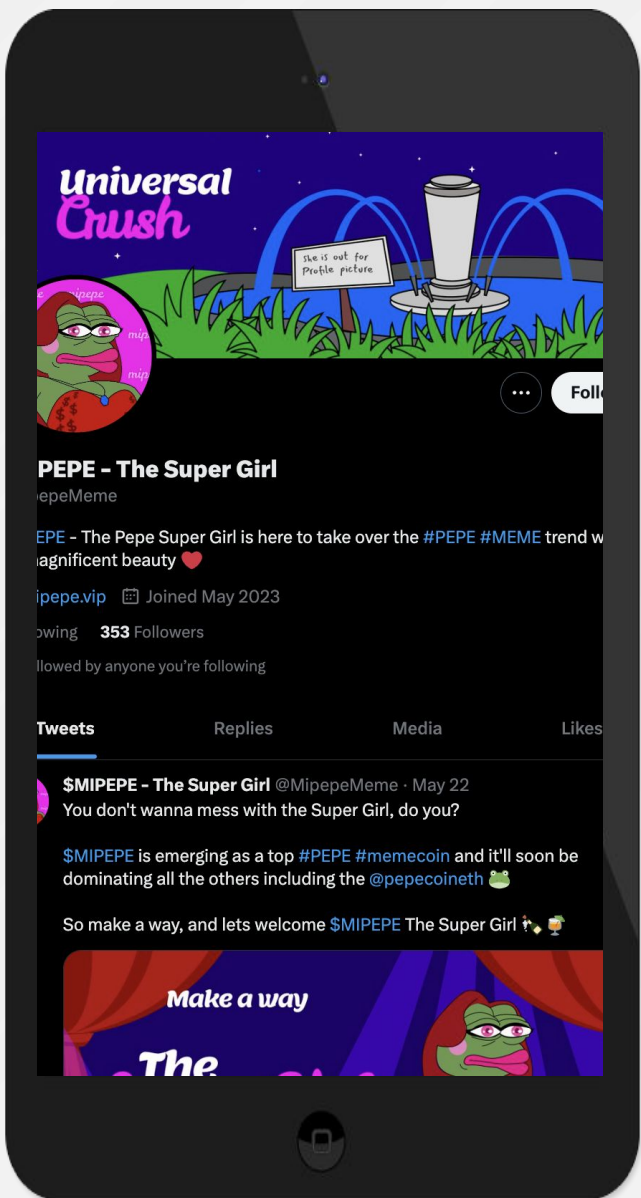


# SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

Project's social media pages are not very active



Twitter

@MipepeMeme

- 352 followers
- 2 posts total



Discord

- Not available



Telegram

@TelegramUSERNAME

- 767 members
- No active members
- No active mods



Medium

- Not available



# SPYWOLF

## CRYPTO SECURITY

Audits | KYCs | dApps  
Contract Development

# ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 500 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to  
[contact@spywolf.co](mailto:contact@spywolf.co) or  
[t.me/joe\\_SpyWolf](https://t.me/joe_SpyWolf)

## FIND US ONLINE



[SPYWOLF.CO](https://spywolf.co)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



[@SPYWOLFNETWORK](https://t.me/SPYWOLFNETWORK)



# Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

## **DISCLAIMER:**

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.